sciendo

Can small businesses remain cyber secure while relying on personal mobile devices?

Renata Karpavičė

Faculty of Public Governance and Business
Mykolas Romeris University
Ateities 20
Vilnius LT-08303, Lithuania
renata.karpavice@gmail.com

Asta Valackienė

Faculty of Public Governance and Business
Mykolas Romeris University
Ateities 20
Vilnius LT-08303, Lithuania
avala@mruni.eu

Abstract: The use of personal mobile devices by SMEs is widespread, but it raises increasingly pressing cyber security issues. Particular attention in this article is paid to the preparedness of small enterprises to guarantee cyber security as personal mobile devices are used in the workplace. This study explores how the use of personal mobile devices impacts cyber security in small businesses and how errors can be prevented when developing a unified model for managing cyber security risks for small and medium enterprises (SMEs). The study employs a descriptive research design, statistical analysis, multiple case studies of cyber security practices in the United Kingdom, Australia, and the United States; analysis of various strategies and standards; modeling and expert assessment (semi-structured interviews). The uniqueness of the proposed model lies combining integrated strategies and recommendations for managing various cyber security risk factors, thereby enabling SMEs to manage these risks using a holistic approach.

Keywords: *cyber security, personal mobile devices, small and medium-sized enterprizes*

https://doi.org/10.2478/bjes-2026-0030 *TalTech Journal of European Studies*, 16(3(46))
Tallinn University of Technology (ISSN 2674-4619)

1. Introduction

While media headlines tend to report only on cyber-attacks on larger companies, more than half of all cyber-attacks worldwide target small and medium-sized enterprises (SMEs). According to the statistics from StrongDM (2024), as many as 75% of SMEs would not be able to continue operating if they were subjected to a cyber-attack involving encryption or ransomware. However, as many as 59% of SME owners do not implement cyber security measures in their businesses because they believe that their companies are too small to be targeted by cyber-attacks.

According to the European Commission data from December 2023, ransomware attacks occur every 11 seconds (European Commission, 2023). According to 2022 data of the Lithuanian National Cyber Security Centre, every second registered cyber incident registered in Lithuania involves an SME, and the number of successful hacking incidents has more than doubled, increasing by 129% (CTAC, 2023). In 2021, Civitta and Telia carried out a survey of businesses and public bodies in Lithuania to assess SMEs' cyber security awareness. The study showed that every second organization surveyed in the study considered protection against cyber hacking and cyber-attacks unnecessary, while only 16–20% expressed an interest in such cyber security measures. According to a study conducted by CISCO Academy, in 2022, despite the increasingly concerning figures, as many as 43% of SMEs had no cyber security plan, while as many as 52% of small and medium-sized enterprises had no IT security experts (CISCO Umbrella, 2022). These statistics demonstrate the relevance of the topic and this study. Lithuania provides a compelling case in this regard because it has demonstrated proactive engagement in improving SME cyber security practices, was among the earliest EU Member States to implement the NIS2 Directive and has invested in dedicated research and awareness initiatives targeting the SME sector (see 'Council directive (EU) 2022/2555', 2022; 'Council regulation (EU) 2019/881', 2019; 'Council regulation (EU) 2021/887', 2021). Lithuania therefore provides a particularly relevant and timely setting in which to examine cyber security challenges faced by SMEs.

Personal mobile devices have emerged as indispensable productivity tools for SMEs, allowing employees to work remotely and collaborate efficiently. However, while the implementation of BYOD (Bring Your Own Device, the practice whereby employees use their personal devices for work purposes) expands opportunities for resource use, it also gives rise to increasingly urgent cyber security concerns.

Systematic literature reviews have identified both external and internal challenges in corporate cyber security management (Jayarao, Ray and Panigrahi, 2024; Ali and Kaur, 2021; Harthy, 2022; Howell *et al*., 2023; Fezzey *et al*., 2023; Chandna and Tiwari, 2023; Mierzwa and Klepacka, 2023; Rathnayaka *et al*., 2023; Sukumar, Mahdiraji and Jafari-Sadeghi, 2023; Wiechetek and Mędrek, 2018; Zuhaira and Ahmad, 2021; Palanisamy, Norman and Mat Kiah, 2021; Benz and Chatterjee, 2020; Downer and Bhattacharya, 2022; Franco *et al*., 2024; van de Weijer, Leukfeldt and Moneva, 2023; Wang, Ho and Shan, 2024).

However, previous studies remain fragmented, and there is a lack of applied research on the use of personal mobile devices in SMEs. Specifically, limited research has addressed the development, modelling, and testing of frameworks for securing SMEs' cyber systems where BYOD is used. It may be argued that these emerging challenges cannot be adequately addressed through conventional organizational management methods alone. New cyber-security management strategies, cyber-security preparedness plans and corresponding measures are therefore needed.

The conceptual analysis and research problem in our study stem from the absence, in both scientific literature and applied research, of a holistic approach to cyber security in SMEs that incorporates multiple criteria and evaluates real practical experience of the risks, challenges, and security implications associated with the use of personal mobile devices.

Given SMEs' constraints in terms of budget, competence, and access to information, the analysis must be broadened. This study addresses this gap by developing and validating a conceptually sound, empirically tested cyber security risk management model for personal mobile devices used in the workplace.

This model can help SMEs navigate the complex process of implementing cyber security practices at all levels of their operations, particularly where personal mobile devices are used under a BYOD policy. To substantiate the conceptual link between the two dimensions—the use of personal mobile devices under a BYOD policy and cyber security management in everyday practices—a general research question (GRQ) was formulated:

GRQ: *How does the use of personal mobile devices affect the cyber security of small businesses, and what cyber security risk management methodology should be applied by SMEs that use personal mobile devices under a BYOD policy?*

Based on the main research question, this study aims to analyze the impact of personal mobile device use on business cyber security and to develop a BYOD risk management model for practical application.

To achieve this aim, the following research tasks were formulated: (1) to conceptualize the theoretical aspects of BYOD-driven personal mobile device use and its implications for SMEs cyber security; (2) to empirically test personal mobile device use in business, the application of BYOD policy, cyber-security practices, relevant legal frameworks, and expert evaluation; (3) to develop and validate the model by implementing good practices, conducting expert interviews, and gathering practical insights into the management of cyber security issues and crises in SMEs.

The paper is structured as follows: Section 2 examines the theoretical aspects of personal mobile device use in relation to business cyber security and addresses the concepts and theoretical framework for ensuring SME cyber security in Lithuania. Section 3 presents the empirical investigation, which applies a combined research strategy, examining good cyber security practice standards, multiple cases of personal mobile device use, and conducting expert interviews through the semi-structured interview method. In Section 4, a unified systematic model of cyber security risk management for personal mobile devices used for work in SMEs is proposed. The final section outlines insights from the theoretical analysis and the empirical investigation and proposes recommendations for future research.

2. Theoretical foundations of cyber security concerning the use of personal mobile devices in small businesses

2.1 The concept and main characteristics of mobile technologies and their impact on small businesses

Mobile technologies are defined in various contexts and cover a wide range of devices, software, and networks designed for mobile use. In examining the concept of mobile technology and its impact, the study focuses on four key characteristics that define mobile technology—mobility, availability, interactivity, and contextuality (Boeckl *et al.*, 2023). These characteristics encompass the capacity of mobile technologies to adapt to the users' environment and needs without limiting this adaptability by the requirements of technological knowledge or imposing restrictions on the presentation and management of information (Ma *et al.*, 2021).

According to *DataReportal* data for January 2024, Lithuania has 2.41 million internet users and 3.24 million mobile users, representing 119.9% of the total population. These figures are based on GSMA Intelligence data and confirm the widespread use of mobile technologies in Lithuania. Also, according to Ookla, average mobile internet speed in Lithuania is 82.53 Mbps, while average fixed internet speed is 103.04 Mbps (*Datareportal*, 2024a; 2024b). Further analysis of the data provided by this source on internet traffic by device shows that laptops and desktop computers account for the largest share (53.10%). Mobile phones account for 46.32% of the traffic and show strong annual growth of 16.9%. Tablet computers account for only 0.57% of the traffic, and their usage has decreased by as much as 54.4%. This may be explained by the highly advanced mobile phone technology, which enables much wider range of functions of this device. These data indicate that Lithuania's level of digitalization is consistent with global trends, with more than three-quarters of the population using social networks, mobile devices outnumbering the population, and almost 90% of the population using the internet. This situation creates particularly favorable conditions for the development and organization of a business model based on mobile technologies.

Globally, and in Lithuania, mobile technologies significantly influence business, with research indicating productivity gains of up to 34% (Ismail, 2017). According to Drazic and Schermuly (2024), the use of mobile devices by remote workers increased particularly sharply during the COVID-19 pandemic. The proliferation of remote working coincided with the rapid development of digital technologies, driving the growth of e-business and the use of collaboration tools. These developments also highlighted the need to ensure flexible and resilient systems, networks, and services in times of disruption.

According to data provided by the Private Finance Online Research Center in their *Research and markets report* (2020), 95% of organizations allowed some form of use of personal devices for work even before the pandemic. Following the onset of the COVID-19 pandemic, 85% of organizations had implemented BYOD policies, according to Mordor Intelligence (FinancesOnline, 2024). Thus, both the growing use of mobile technologies in business and the increasing adoption of personal devices in organizations through the implementation of BYOD policies, create significant risks of cyber security incidents that occur when personal devices connect to the organization's networks and systems.

According to the *Cost of a data breach report 2023* by IBM Security in 2023, smaller organizations incurred substantially higher costs from cyber security incidents related to data breaches than they had in 2022. The study revealed that for organizations with fewer than 500 employees the average impact of cyber incidents involving data breaches increased by 13.4%, from 2.92 million to 3.31 million US dollars (IBM Security, 2023).

Research company Research and Markets (2025) estimates that the global market for organizations adopting BYOD policies to support their business activities and staff mobility needs is worth 98.8 billion US dollars. Experts expect the figure to reach 157.3 billion US dollars by 2026, equivalent to an annual growth rate of 16.7% (Research and Markets, 2025). These data support the assumption that the application of the BYOD policy will remain relevant and continue to increase. Notably, BYOD is a central aspect of business mobile technology use, allowing employees to work on personal devices, access networks, and handle confidential data. According to Rathnayaka *et al*. (2023), a comprehensive, clear, and employee-friendly policy can provide tangible business benefits by reducing equipment acquisition costs, increasing employee productivity and job satisfaction, and providing greater flexibility and mobility. However, integrating personal and work data on the same device increases the risk of accidental data leakage or unauthorized access, while device loss or theft may compromise organizational confidentiality. Also, the use of unauthorized applications and devices in disregard of cyber security requirements or the organization's cyber security procedures, together with insufficient training of employees in the safe use of personal mobile devices, can contribute to errors resulting in cyber security incidents (Chandna and Tiwari, 2023).

The use of employees' personal mobile devices in the workplace creates a complex security environment for organizations because devices differ by manufacturer, configuration, model, and even age. Researchers (Ganiyu and Jimoh, 2018; Benz and Chatterjee, 2020; Harthy, 2022) have identified risks and threats associated with the application of the BYOD policy when analyzing risk management systems. Organizations applying a BYOD policy should regularly review their access policy and continuously reassess their BYOD security needs: that is, they should maintain control over processes, equipment, software and user devices, as well as user behavior (Blanton, 2025). Meanwhile, the widespread adoption and growing use of mobile devices create new cyber security challenges, making such devices attractive targets for cyber criminals. Therefore, organizations of any size or sector must adapt their cyber security strategies to address these evolving and growing threats.

2.2 Application of the legal framework for ensuring cyber security of small businesses in Lithuania

Cyber security regulation in Lithuania is based on EU directives, regulations, and national legislation. A review of numerous legal documents on cyber security in Lithuania shows the growing importance of understanding the necessity and uniqueness of the applicable legislation. The main legal acts regulating cyber security in Lithuania are: (1) the *Law on Cyber Security of the Republic of Lithuania 2014* (No. XII-1428, updated in 2024 by implementing the European Union NIS2 Directive); (2) the *Law on the Management of State Information Resources of the Republic of Lithuania 2023* (No. 2023-26025); (3) the *Law on Electronic Communications of the Republic of Lithuania 2021* (No. 2021-24230); and (4) the *Law on Legal Protection of Personal Data of the Republic of Lithuania 2024* (No. XIV-2626). Notably, SMEs need to self-assess not only whether a specific legal act is applicable to them, but also which compliance risk management measures are necessary to avoid penalties and legal liability arising from non-compliance.

In 2020, the Ministry of National Defense of the Republic of Lithuania published the guidelines *Cyber security guide for business 2020*. These guidelines were developed to enhance cyber security awareness among SMEs and to assist managers in understanding related challenges and risks, while providing recommendations and best practices for effective risk management (Ministry of National Defence (Lithuania), 2020). The main recommendations in this report highlight the need for businesses to self-assess their processes and systems and determine what information they manage and process. It remains important to identify cyber security threats and their sources, along with potential vulnerabilities in systems or processes. After identifying cyber security threats, businesses must self-assess the associated risks and potential impacts before implementing measures to manage those risks and mitigate their effects.

However, the recommended good security practices in this report only briefly mention the application of the BYOD policy and the need to distinguish between the use of personal and work equipment. The principal recommendation focuses on defining access rules for employees' personal devices and using mobile device management services.

3. Experiences of good cyber-security practices in personal mobile device use: A research review

3.1 Empirical evaluation of cyber security and risk management related to the application of a BYOD policy in SMEs

3.1.1 Justification for the expediency of the research

Previous studies suggest that environmental uncertainty may create new cyber security challenges within corporate entities. Both the growing use of mobile technologies in business and the expanding use of personal devices in organizations through BYOD policies create significant risks of cyber security incidents occurring when such devices connect to organizational networks and systems. However, many practical questions remain unanswered: What happens to small-business cyber security when work becomes both mobile and personal? Does Bringing Your Own Device also mean bringing your own risk? In terms of lessons for small businesses: when small businesses adopt BYOD, what could go wrong? Answering these questions requires more thorough analysis and a comprehensive perspective on SME cyber security.

Hence, we propose the following hypothesis:

H1: *The application of a BYOD policy in Lithuanian SMEs without an appropriate cyber security risk management model increases enterprises' vulnerability to cyber threats.*

The hypothesis correlates with the scientific problem and the general research question (GRQ) to determine *what cyber security risk management methodology should be applied by SMEs that use personal mobile devices and apply a BYOD policy?* It is also consistent with the research aim—to examine the impact of BYOD policy implementation on the cyber security of SMEs in Lithuania and to develop a theoretical cyber-security risk-management model for SMEs applying a BYOD policy.

Drawing upon a review of the scientific literature of these social phenomena, this study employs an exploratory research design. The identified research problem allows us to analyze the area of cyber security for SMEs, considering the interaction of multiple criteria, and to explore practical experiences across different countries. Following an emergent research approach, the authors chose a qualitative research methodology to provide empirical insight into the social phenomenon analyzed, comprising multiple case studies that examine

experiences of good practices of cyber security risk management in the UK, Australia, and the USA, as well as semi-structured interviews with cyber-security experts in Lithuania to capture the complexity and depth of cyber security processes associated with the implementation of BYOD policies in small businesses. Purposive sampling, a non-probability sampling strategy, was applied to analyze case studies that represent examples of good practice. For the semi-structured interviews, experts (N = 9) were selected through criterion sampling based on their long-term professional experience in cyber security within the Lithuanian business environment.

Thus, the study discusses several case studies illustrating global practices, while the expert assessment reflects the situation in Lithuania and provides a detailed analysis of the phenomenon, which allows drawing general conclusions.

Table 1. Research tools.

Research stages	Research criteria (1-3) and indicators (1-8)	Methods of analysis
1st stage: Theoretical background of the research; the concept of mobile technologies and their influence on business organization, cyber threats to SMEs, the application of legal base of requirements to ensure the cyber security of SMEs in Lithuania, and good practices of cyber security in different countries.	*1. Mobile technologies in the organization of small businesses.* 1) The concept of mobile technologies and their impact on the cyber security of SMEs and risk management processes. 2) Identification of cyber threats to SMEs. 3) Identification of the application of the legal framework for ensuring SME cyber security in Lithuania. 4) Comparison of cyber security practices in Lithuania and international standards.	Systematic literature analysis. Analysis of secondary statistical data. Semi-structured interviews.
2nd stage: Organization of the empirical research. Practical experiences and expert evaluation of the cyber security situation and risks when SMEs allows to use personal mobile devices for work.	*2. Identification of the risks of using personal mobile devices for work in SMEs and their management practices.* 5) Identification of the risks of using personal mobile devices for work in SMEs and their management practices. 6) Identifying recommendations for cyber security and risk management processes through different global practices.	Systematic literature analysis. Multiple case studies. Semi-structured Interviews.
3rd stage: Construction and verification of the model. Significance and practical applicability.	*3. A cyber security risk management model for SMEs using personal devices under BYOD.* 7)Justification of the structure and interaction of the elements of the model. 8)Verification of the model performance/ perspectives for the application of the model.	Systematic literature analysis. Analysis of secondary statistical data. Semi-structured Interviews. Modelling.

This article aims to answer the following specific questions:

RQ1: *What cyber security challenges do small businesses face when using personal mobile devices?*

RQ2: *How does the use of personal mobile devices affect cyber security in small businesses?*

RQ3: *What lessons about cyber security have small businesses learned from using personal mobile devices?*

3.1.2 Data sources

To complete the methodology of this study, detailed research instrumentation was developed around three criteria, which are empirically verified by enabling eight indicators (presented in Table 1).

The proposed research tools highlight important aspects of the transformation of cyber security in SMEs, establishing the principal dimensions of the empirical analysis.

3.2 Data analysis

3.2.1 Multiple case studies of BYOD policy recommendations

According to the *Cyber security breaches survey 2025* by the UK National Cyber Security Centre, SMEs in the UK have improved their cyber security hygiene: 48% of companies conducted cyber security risk assessments, compared with 41% in 2024; 62% of companies had cyber insurance, compared with 49% in 2024; 59% of companies had a cyber security policy, compared with 51%; and 53% of companies had business continuity plans, compared with 44% in 2024. Overall, the experience of the UK underlines the need for organizations to balance technical and organizational controls when they do not have full control over end-user devices, particularly where organizations allow the use of personal mobile devices and apply the BYOD policy. (National Cyber Security Centre UK, 2020)

The Australian Cyber Security Centre (2024) recommends implementing the Essential Eight strategy to strengthen the cyber security of an SME. This strategy comprises the following recommended technical cyber security measures: program updates; operating system updates; multi-factor authentication; restricted rights of the administrator; control of applications; limiting Microsoft Office macros; strengthening the security of user access; and regular backups. In summary, Australian authorities highlight the value of a multi-layered approach to cyber security, encompassing BYOD policies, technical controls, continuous staff training, incident response, and strict compliance with privacy laws (Australian Cyber Security Centre, 2023).

In 2024, the US Department of Defense presented a new document entitled *CIS Controls implementation guide for small- and medium-sized enterprises (SMEs)* (Center for Internet Security, 2017). The guidelines present a three-step approach to the deployment of cyber security practices. The first stage is knowledge: the identification of devices and software present on the organization's network and an understanding of its cyber security baseline. The second stage focuses on implementing a basic level of organizational security through employee education and measures designed to prevent cyber security events. In the final stage, the organization must prepare in advance for cyber security risk events.

To summarize the recommendations on BYOD policies from the UK, Australia, and the USA: SMEs in these countries face comparable cyber security risks linked to vulnerabilities and limitations in their risk management capacity.

3.2.2 Analysis of semi-structured interviews

Data obtained from the multiple case studies were examined alongside evidence from semi-structured interviews with cyber security experts in Lithuania, enabling triangulation of information and its effective application in Lithuania. Based on the research questions, the interviews were structured around three scenarios, allowing the interview questions to be divided into three parts: approach; threats and risks; and practice. All interviews were carried out over a one-month period in March and April 2025. Each interview was conducted via remote video conference with each session lasting approximately 45–60 minutes. Interviewees were purposively selected on the basis of certified qualifications and substantial professional experience in cyber security, including senior executives and managers. Selection criteria included professional role, specialization, SME engagement, policy expertise, and familiarity with mobile technologies and the associated threats.

Representativeness and reliability of participant selection. The validity of expert opinions and assessments is considered sufficiently high when 9 (nine) experts are included in the study. Beyond this point, the accuracy of expert decisions and assessments increases only marginally. To protect the identity of the informants, as required by research ethics, participants were assigned the code E ("expert"). Informants' responses (N = 9) were coded as follows: E1, …, E9.

Composition of the expert panel. The panel comprised heads of cyber security centers and cyber security risk management companies (E1, E2), heads

of information security services and heads of IT departments at higher education institutions (E8, E9), cyber security officers (E3, E5, E7), a cyber security expert from an SME (E4), and the head of the Cyber Threats Department at the National Cyber Security Centre (E6).

Structure of the interview protocol. All interviews opened with a couple of exploratory and rapport-building questions intended to help interviewees feel at ease and avoid cognitive bias. *The first section* comprised closed-ended questions about the experts' experience in the field of cyber security and with SMEs, with responses recorded on a 5-point Likert scale. *The second section* comprised the evaluation of the situation—the experts' opinion on the cyber security situation and awareness of SMEs—and also discussed the importance of cyber security practices. The evaluation questions were presented on a 5-point Likert scale, on which experts indicated their degree of agreement or disagreement with statements concerning a particular point of view, object, person, or event. The scores were aggregated across all statements to obtain an overall measure of the respondents' point of view. *The third section* consisted of ten open-ended questions, in which the experts were asked about the cyber security situation in SMEs in Lithuania and their approach to cyber security, the risks associated with implementing a BYOD policy in SMEs, preparedness to manage these risks, technical and organizational control measures, recommendations how to manage incidents, and recommendations for BYOD policy development.

A logical matrix of a semi-structured interview was developed (see figure 1).

The audio-recorded interviews were transcribed verbatim, allowing analysis of the transcripts. All informants were asked to review the findings and provide comments.

Coherence of expert opinions. The analysis of the interview data began with an assessment of the statistical consistency of expert opinions. According to Podvezko (2005), the results of expert assessments can be applied in practice if a sufficient level of consistency among expert opinions has been established. The quantitative assessment of the consistency of expert opinions was performed using Kendall's coefficient of concordance (W). This coefficient reflects the ratio of the variability of the overall assessment of the objects being assessed to the maximum possible variability of the overall assessment. If the experts' opinions are consistent, the value of Kendall's coefficient of concordance W is close to 1; if the assessments differ substantially, the value of W is close to 0 (Podvezko, 2005).

Kendall's coefficient of concordance (W) was calculated using the Statistical Package for Social Sciences (SPSS), version 30. Since only scaled expert assessments were relevant to the calculation, only questions with rating scales in the *second part of the interview list* (Question Block 1, containing eight statements, and Question Block 2, containing ten statements) were included in the calculation of the coefficient. The remaining questions in the questionnaire were open-ended and therefore excluded from the calculation of the concordance coefficient. The result of the Kendall concordance coefficient in total was $W = 0.637$ and the maximum mean/average equaled 4.966. Based on Kendall's coefficient of concordance ($W = 0.637$), it is concluded that the experts' opinions were sufficiently consistent.

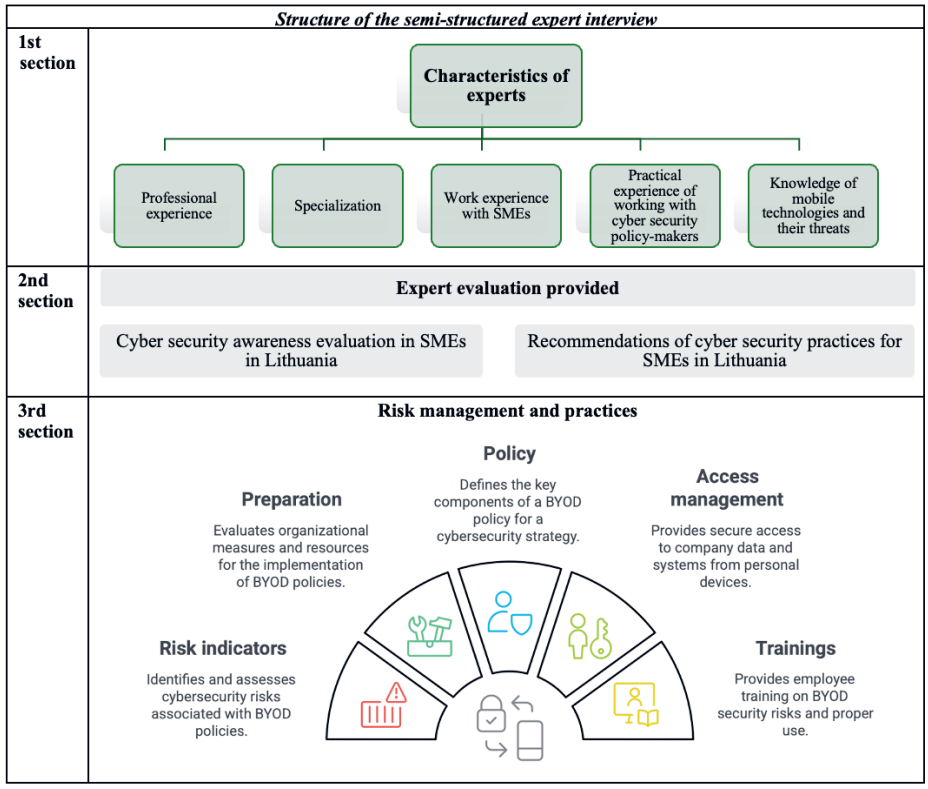


Figure 1. The logical matrix of a semi-structured interview.

The authors then examined what experts think of the state of cyber security in Lithuanian SMEs and the importance they attributed to recommended cyber security practices in these companies. The experts discussed eight statements concerning the significance of cyber security practices for SMEs,

employee awareness and preparedness, approaches to assessing cyber security risks or gaps, the importance of the functioning of IT systems for SME operations, etc. They provided their assessments on a 5-point Likert scale, ranging from 1 ("strongly disagree") to 5 ("strongly agree"). The ratings were then converted into ranks across all eight statements, and the level of agreement among experts was analyzed using Kendall's coefficient of concordance (*W*). The mean rank values ranged from 1 to 8, with higher values indicating that experts collectively placed that statement at a higher position of importance or agreement relative to the others. The mean rank of each statement was as follows: "Cyber security is important for SMEs"—5.50; "SMEs are well prepared to respond to cyber incidents"—2.06; "SMEs see the benefits of, or need for, cyber security measures"—3.67; "Existing cyber security measures are too expensive for SMEs"—3.00; "A cyber incident would have a significant impact on SMEs"—5.94; "SMEs can become victims of a cyber incident"—7.17; "The functionality of IT systems or electronic services is very important for SME operations"—6.28; "SMEs know how to assess cyber security risks or gaps"—2.39.

Next, the experts were asked to assess the cyber security practices they would recommend to SMEs on a 5-point Likert scale ranging from 1 ("not important at all") to 5 ("very important"). Each of the ten practices was evaluated according to its mean rank, where a higher mean rank indicates greater relative importance assigned by experts compared to the other practices. The mean rank for each practice was as follows: "Password policy"—5.39; "Multi-factor authentication (MFA)"—7.06; "Cyber security training for employees"—6.33; "Vulnerability assessment and penetration testing (VAPT)"—4.17; "Regular backup creation"—5.83; "Privileged access management (PAM)"—5.50; "Network segmentation"—3.56; "Incident management plan"—5.61; "Data encryption"—5.72; "Cyber security audit"—4.83.

The experts indicated that SMEs rate their preparedness to respond to cyber incidents very poorly. They also assessed SMEs' capacity to assess cyber security risks or vulnerabilities independently to be weak and insufficient.

In the *third part of the interview*, which comprised open-ended questions, the experts were asked to share their experience in assessing cyber security risks in SMEs and to evaluate aspects of BYOD policy implementation in SMEs.

When analyzing the benefits and risks of implementing a BYOD policy, the experts emphasized that the main risks associated with the use of personal

mobile devices for work are the following: company data leakage and breaches of confidentiality; malicious software such as spyware, malicious encryption software, ransomware, viruses, and similar threats; insider fraud when an employee deliberately removes company data; insecure network connections, such as public, open Wi-Fi networks; the physical loss of a personal device containing company data; use of insecure software; device vulnerability through visiting unsecure websites; and failure to keep devices and security solutions updated. The experts emphasized that SMEs should assess their readiness to implement a BYOD policy, considering their available IT resources, employee competencies, and the management of compliance risks. They highlighted the following key elements of the BYOD policy that SMEs need to engage in their cyber security strategy: staff training that clearly defines permitted and prohibited uses of personal equipment; procedures for preparing and inspecting personal equipment before it is used for work; the scope and objectives of the use of technical security solutions; maintenance and support requirements for the installation of personal equipment and security upgrades; regulation of access to company systems and data; the scope and procedure for monitoring personal mobile devices; procedures for reporting the loss of personal equipment and ensuring data protection; the respective responsibilities of the organization and the employee, including the limits of those responsibilities; and procedures and responsible personnel for updating and maintaining the policy.

The experts identified the following key recommendations for effective staff training: training should be both theoretical and practical; create value and be tailored to the role of the employees; training should be inclusive; based on real-world examples; take place regularly, for example, quarterly; incorporate simulations, such as phishing simulations, that should be performed continuously; the knowledge acquired during the training should be assessed during the tests; and training should cover broader topics on cyber security and cyber security hygiene.

The experts also identified the following measures to be taken when an employee loses a personal device containing company data: a clearly defined procedure specifying who has to report the loss, when it must be reported and how; appointing a person responsible for managing such incidents; a clear procedure for assessing the potential damage caused by an incident (including whether data have been lost or may be disclosed); where necessary, notifying the relevant authorities of a potential data breach; and access to the procedures for blocking or wiping the device of the lost person, deleting the data it contains.

Table 2. Triangulation of the semi-structured interview content analysis.

Criteria	Category, subcategory, and indicators reflecting them	RR*	Interview quotes
Policy and governance	The policies define objectives, scope, security measures, their extent, and company and employees' responsibilities	6	"...first of all, a very clear instruction should be written"
		7	"...a clear definition of what is allowed and what is prohibited due to the use of personal equipment"
		6	"...what privileges these people have when working with these personal devices"
	Scope, objectives and procedure for cyber security monitoring actions.	6	"...mobile equipment management requirements and conditions that define the use of those devices"
		8	"...if a device does not meet certain requirements of the standard, versions and other things, it simply does not allow that device to access the organization's data"
	Data protection and privacy and company data protection procedure.	5	"...there is no doubt that endpoint monitoring"
		4	"...inform the original person that it would be possible to simply block the device in its entirety"
Risk assessment	Self-assessment of cyber security risks.	9	"…data breaches"
		2	"...say I'm backing up with company data, leaving the company, buying another machine and recovering the data"
		5	"...and then you use it everywhere else in cafes, airports"
		9	"...physical loss"
		5	"...cannot be controlled mainly by device, security and application update"
	Overall self-assessment of the organization in terms of IT resources and staff competence and compliance risks.	5	"...do you have an IT employee and do you have a smart IT employee? "
		5	"...staff must be instructed on how to use the "container""
		3	"...should first make a risk assessment of the company"
Controls	Technical security measures must be installed and configured before allowing access to the company's resources.	9	"...MDM solutions"
		7	"...Of course, a VPN or any other gateway"
		7	"...antimalware, antivirus and others"
		4	"...This is a multifactor, strong passwords"
		5	".... as long as the device is connected to the enterprise, it follows the enterprise policy"
		5	"...if you do not have the latest software, access to all company resources should be restricted in general"
Training	Training of employees and its organization combine theory and practice in an inclusive form, based on real examples, with knowledge tested regularly.	9	"… including devices in certain training campaigns, such as phishing simulations. "
		4	Training must be value-creating and tailored to the role of employees.
		6	"...just take some real-life scenario to show what can happen"
		7	"...create periodic training to quarterly one"
		7	"...those trainings would be mandatory for all staff. "
Incident management	Incident management in case of device loss or cyber security breach through well-defined procedures, action sequences, and assignment of responsible persons.	5	"...The worker should know in advance what to do when losing, whom to contact, whom to inform. "
		4	"...to see if I have to report there to the other authorities involved, the data protection inspectorate and the police. "
		9	"...this remote access is probably possible to remove. The data has then been removed from that access at a distance. "
Indicators for enhancing BYOD policy	The effectiveness of policy implementation is evidenced by metrics including the number of cyber incidents, the share of trained employees, and outcomes of phishing simulations.	9	"...Basically, some indicator of cyber security incidents."
		6	"...Training would also be one of the indicators for me. "
		4	"...Phishing or other simulations are performed and how many of these people have passed without success"
		5	"...how many, what percentage of devices meet the security criteria and are used as BYOD"

* Repetition rate

The experts outlined indicators that SMEs should monitor to ensure effective implementation of BYOD policies. The main indicator highlighted by the experts was the number of cyber security incidents, considering their scale and significance, which should also be defined in the BYOD policy. Other indicators included the number of employees who successfully completed training; phishing simulation results; the functioning of devices that meet the technical security requirements specified in the company's systems; and the number of requests to use personal devices for work.

The authors therefore applied a systematic research approach based on interpreting the interview data, using qualitative content analysis triangulation according to the research criteria and six interview scenarios: policy and governance, risk assessment, control, training, incident management, and BYOD policy improvement indicators, as well as data from legal documents.

The triangulation of the semi-structured interview findings is presented in Table 2.

The interview findings validated the effectiveness of cyber security measures in applying BYOD policies in SMEs and highlighted the pursuit of sustainable competitive advantage and opportunities to participate in business ecosystems.

4. A unified systematic model: creation and application

The conceptual and empirical analyses of the phenomenon led to the development of a unified systemic model that adopts a holistic approach to the application of a BYOD policy in SMEs to ensure cyber security and indicates how to manage risk.

The development of the model was based on:

1) Porter's (1985) classical value-chain methodology, according to which input data are processed, modified, and modeled within a business system until a change is achieved—the output result;
2) the identification of factors that determine the model input, the starting point of the activity, and the output generated by the model (Aytulun and Guneri, 2008);

3) a structured approach to design, implementation, monitoring, and improvement (Wiechetek and Mędrek, 2018);
4) the five general phases of business process modelling (Zuhaira and Ahmad, 2021);
5) the recommendations of the Australian Cyber Security Centre's 4Ps (Purpose, Planning, Policy, and Performance); and
6) USA CISA's emphasis on developing a culture of cyber security within the organization to mitigate the risks of a BYOD environment (CISA, 2021).

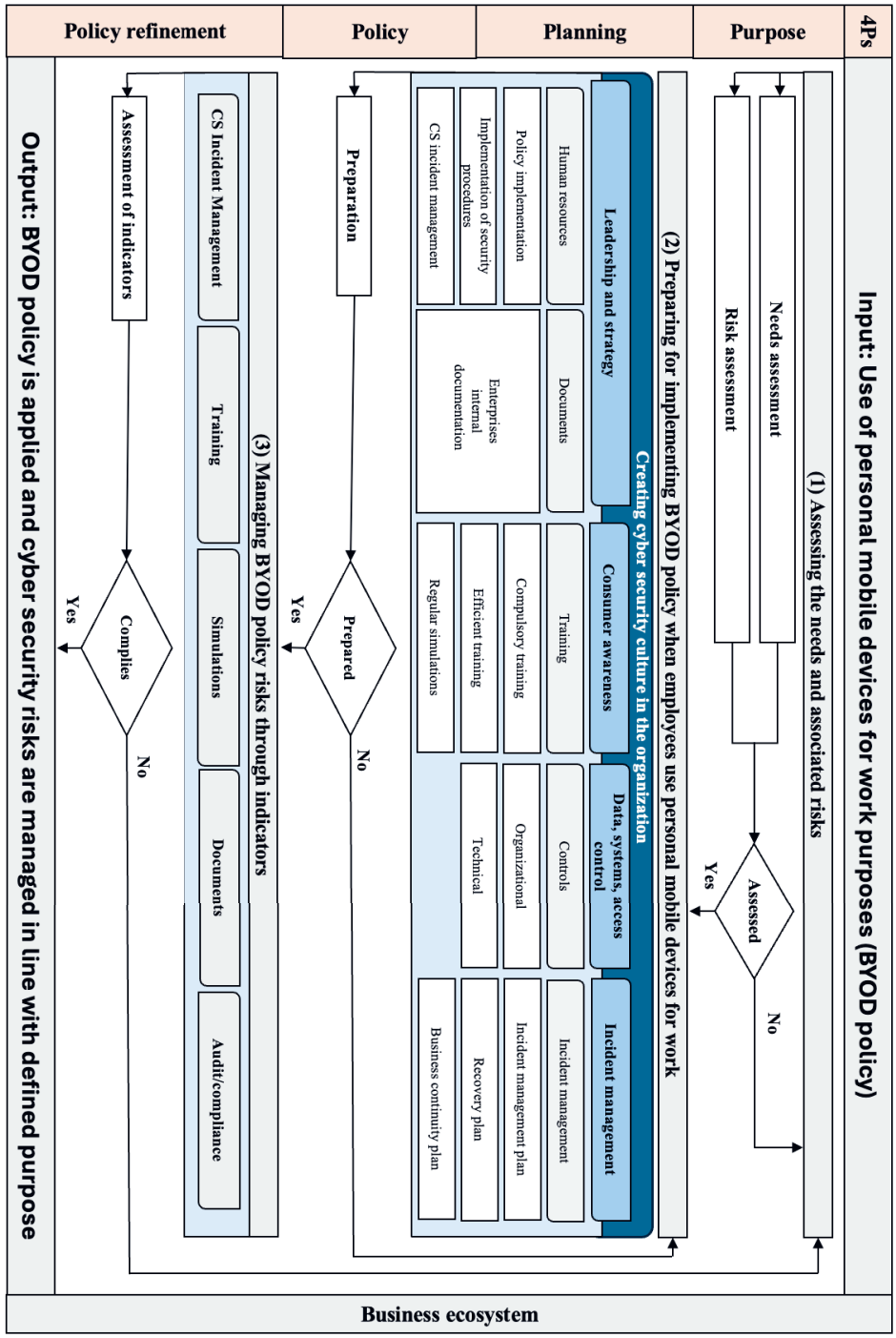
The design of the model for applying a BYOD policy to cyber security risk management in SMEs is based on theoretical insights and empirical data, including good global practices and semi-structured expert interviews. The structure of the model reflects its cyclical nature (Levels 1–4) and close interaction. The model interacts with these structural components, representing risk assessment and management processes. The approach here is based on the fact that the model operates as a cycle.

The model is visualized in figure 2.

The logical construction of the model. The starting point of the model is understanding the effective use of personal mobile devices for work in SMEs (under a BYOD policy), responding to and following the segments and phases of business process modeling (input, business system expression, output, and the achieved result). This is followed by assessing the need and associated risks (Level 1: Input and self-assessment) requiring companies to assess the needs and risks associated with the application of the BYOD policy, considering the cost-benefit balance before deciding whether to adopt the BYOD policy.

The self-assessment should address the following questions: Is it possible to achieve the company's goals without using personal mobile devices for work? Does the company have sufficient IT resources to ensure the cybersecurity of its systems when personal mobile devices are used for work? Can the company manage the risks created by the use of personal mobile devices for work? Do the company's employees have sufficient competencies to ensure cyber security when using personal mobile devices for work? Does the company have the tools and capabilities required to protect the company's data and information when using personal mobile devices for work?

Figure 2. Cyber security risk management model for the use of personal mobile devices for work in SMEs



It is also recommended that companies assess the risks associated with the implementation of a BYOD policy by answering the following questions: How will the company ensure the prevention of data leakage and breaches of confidentiality? How will it protect its systems against malware such as spyware, malicious encryption tools, ransomware, and viruses? How will the company manage the risk of insider fraud when an employee intentionally removes company data? How will it prevent personal mobile devices from connecting to insecure networks, such as public, open Wi-Fi? How prepared is the company to respond to incidents when a personal mobile device with company data is lost? How will the company ensure that insecure software is not used on personal mobile devices used for work? How will it protect devices if employees visit insecure websites? How will the company ensure that personal mobile devices and cyber security solutions are updated in a timely manner?

Level 1 directly correlates with Level 2, which ensures the preparedness for the implementation of a BYOD policy (Level 2) and demonstrates the efficiency of creating a cyber security culture in the company through the following four components: leadership and strategy; consumer awareness; data systems; and access control and incident management. At Level 2, the model shows the interaction with different subsections of preparedness for the BYOD policy implementation actions variables, including human resources, security procedures, documentation, training, control, and preparation of an incident management plan based on cooperation and evidence, innovative solutions, digital regulation, an integrated ecosystem, and protected privacy of data.

The model then introduces a new dimension, risk management (Level 3). At this level, it requires managing BYOD policy risks which covers the assessment of indicators, including the analysis of cyber security incidents, training of employees, simulations of cases on cyber security and risk management, documentation all procedures, and auditing. For effective risk management, a BYOD policy requires continuous updating of indicators that reflect the effectiveness of policy implementation and risk management, together with monitoring and evaluation of the results.

Finally, the model integrates the output stage (Level 4), where after successfully completing all the preceding stages and carrying out continuous monitoring and control, the company applies a BYOD policy and manages cyber security risks in accordance with the set objectives.

It is worth emphasizing that the hypothesis of this study was essentially validated. Statistical data on SME cyber-attacks demonstrated the vulnerability of companies that lack active security measures, the global best practices confirmed their exposure to risks, and the expert evaluation supported our hypothesis that companies must be prepared to manage crises resulting from BYOD policy implementation.

Therefore, the proposed model, *Cyber security risk management for the use of personal mobile devices for work in SMEs*, has clear practical value.

In summary, the authors demonstrated that the model is based on a continuous risk management process. When business models shift, organizational functions expand, or cyber incidents occur, it is essential to evaluate whether BYOD performance indicators meet policy objectives, and in case of discrepancies, to return to the initial stage to reassess its needs and risks, and implement corrective measures as required.

The novelty of the model is considered from two perspectives: first, at the conceptual level, as a new scientific idea, as there is no systematic model in scientific literature that is designed for SMEs and ensures cyber security when companies try to implement a BYOD policy; and second, our study shows practical relevance, as it helps answer the research question from a practical point of view. The proposed model may also serve as a guiding framework in building the research models for the new studies of cyber security in SMEs in the future.

5. Discussion and conclusion

This study embarked on a journey to develop and empirically evaluate a cyber security risk management model tailored to SMEs, with an aim to navigate the complexities of adopting cyber security and risk management practices across all operational levels. The conclusions drawn reflect the research questions and the objectives established in the study. The literature analysis, review of applied research, multiple case studies, and interviews with experts of Lithuanian cyber security companies and the public sector provided insight into the multifaceted dimensions of effective risk management, the application BYOD policy and work practices, and the important role of leadership in facilitating these processes within the context of SMEs.

The theoretical aspects related to the impact of personal mobile device use for work on the cyber security of SMEs, a list of recommendations, as well as several case studies have shown the relevance of analyzing this social phenomenon. The list of controls established in international cyber security standards and the accompanying *Cyber security guide for business 2020*, issued in Lithuania (Ministry of National Defense (Lithuania), 2020), provide exhaustive guidance that is generally applicable to SMEs, but it could be argued that the information provided may be difficult for SMEs to understand due to technical terminology and complexity.

A review of multiple case studies of cyber security practices among SMEs in the UK, Australia, and the USA suggests that the implementation of a BYOD policy in SMEs is highly variable, there is no one-size-fits-all approach, and that various strategies are needed. According to the analysis of cyber security practices in the UK, Australia, and the USA, SMEs tend to use informal—that is, verbal agreement-based—BYOD policies. While the countries examined have different cyber security practices and rely on different cyber security standards, all practices include basic organizational and technical controls, policy documentation, training, and incident management. It is important to note that the principal focus of the country-level recommendations for the application of BYOD policy differs: The UK emphasizes balanced organizational and technical controls; the USA emphasizes the development of a cyber security culture within the organization; and Australia emphasizes the need for a 4Ps strategy (purpose, planning, policy, and policy refinement).

Based on the analysis of semi-structured expert interviews, it was found that SMEs should first assess their needs and risks before implementing a BYOD policy, using a structured self-assessment questionnaire. The main priority is the protection of company data and personal privacy, which must be ensured by a balance of technical and organizational controls. Effective training that raises employees' cyber security awareness can be said to be an integral part of a BYOD policy. To manage expectations and define the responsibilities of both the organization and its employees, it is necessary to document the BYOD policy.

The proposed model of cyber security risk management for personal mobile devices used for work in SMEs can be applied in two circumstances: (1) the model may be used as soon as the organization considers whether to allow the use of personal mobile devices for work and (2) when the organization already permits the use of personal mobile devices for work.

Because the model incorporates the integrated 4Ps strategy and an organizational cyber security culture, it may be applied in narrower scope depending on the size and activities of the company while retaining essential elements: establishing BYOD policy objectives alongside risk self-assessment; ensuring preparedness through proportionate planning, resources, and policy tools; and establishing indicators for evaluating the effectiveness and compliance of the policies in place. Within the organization, the implementation of the model should be reviewed on a regular basis, in line with changes in the company's operations or in the event of a cyber security incident. Regular monitoring and evaluation of the defined indicators would also help ensure the effectiveness of BYOD policy implementation in the SME.

The model stands out for its holistic approach to shaping cyber security practices in SMEs and is not limited to technical or organizational cyber security assurance controls.

The authors propose that future research should include a longitudinal study, extending the geographical scope of the research to obtain a broader understanding of this social phenomenon and to incorporate experiences and new perspectives from different countries.

The authors' future research will assess the generalizability of the proposed model across different cultural contexts and types of companies. It will examine how regional and sector-specific factors influence cyber security processes in SMEs implementing a BYOD policy and will provide additional empirical substantiation for the proposed model. To achieve these objectives, the geographical scope of the investigation will be broadened to include various European countries. A quantitative research strategy will be employed to further evaluate the effectiveness of the identified cyber security strategies and practices. The research team anticipates that the subsequent studies will engender a more nuanced understanding of the complexities inherent in the field of cyber security and that future research will contribute significantly to the continuing refinement and evolution of BYOD policy implementation in various companies.

Renata Karpavičė is a PhD candidate in information systems and cyber security management at Mykolas Romeris University, Lithuania, and the head of Transparency in the Business Resilience Department at a leading Lithuanian enterprise. Her work integrates over a decade of

professional expertise with research interests in cyber security, digital fraud prevention, and organizational resilience.

Asta Valackienė, PhD in social sciences (sociology), is a professor at the Faculty of Public Governance and Business of Mykolas Romeris University, Lithuania. Her research interests include methodology of science and research, change and crisis management, resilience, and cyber security. Has authored and co-authored research studies, books, handbooks, and has published over 100 scientific papers.

References

Ali, Md.I. and Kaur, S. (2021) 'Next-generation digital forensic readiness BYOD framework', *Security and Communication Networks*, 2021, article 6664426. Available at: https://doi.org/10.1155/2021/6664426

Australian Cyber Security Centre (2023) *Cyber security and Australian small businesses: results from the Australian Cyber Security Centre Small Business Survey*, 2023/BYOD101. Available at: https://www.cyber.gov.au/sites/default/files/2023-03/2023_ACSC_Cyber%20Security%20and%20Australian%20Small%20Businesses%20Survey%20Results_D1.pdf (Accessed: 19 September 2025).

Australian Cyber Security Centre (2024) *Essential Eight explained*. Available at: https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight/essential-eight-explained (Accessed: 19 September 2025).

Aytulun, S.K. and Guneri, A.F. (2008) 'Business process modelling with stochastic networks', *International Journal of Production Research*, 46(10), pp. 2743–2764. Available at: https://doi.org/10.1080/00207540701543601

Benz, M. and Chatterjee, D. (2020) 'Calculated risk? A cybersecurity evaluation tool for SMEs', *Business Horizons*, 63(4), pp. 531–540. Available at: https://doi.org/10.1016/j.bushor.2020.03.010

Blanton, S. (2025) 'What are NIST's mobile device management guidelines?' *JumpCloud*, 18 March. Available at: https://jumpcloud.com/blog/nist-mdm-guidelines (Accessed: 19 September 2025).

Boeckl, K., Grayson, N., Howell, G., Lefkovitz, N., Ajmo, J., Craft, R.E. *et al.* (2023) *Mobile device security: Bring Your Own Device (BYOD)*. NIST Special Publication 1800-22, volume A. US Department of Commerce. Available at: https://doi.org/10.6028/NIST.SP.1800-22

Chandna, V. and Tiwari, P. (2023) 'Cybersecurity and the new firm: surviving online threats', *Journal of Business Strategy*, 44(1), pp. 3–12. Available at: https://doi.org/10.1108/JBS-08-2021-0146

CISA (2021) 'Cyber guidance for small businesses', *Cybersecurity & Infrastructure Security Agency*. Available at: https://www.cisa.gov/cyber-guidance-small-businesses (Accessed: 19 September 2025).

Cisco Umbrella (2022) *Which cyber-attacks most commonly target small businesses?* Available at: https://umbrella.cisco.com/blog/which-cyber-attacks-most-commonly-target-small-businesses (Accessed: 19 September 2025).

'Council directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)' (2022) *Official Journal* L 333, 27 December, pp. 80–152.

'Council regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act) (Text with EEA relevance)' (2019) *Official Journal* L 151/15, 7 June, pp. 15–69.

'Council regulation (EU) 2021/887 of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres' (2021) *Official Journal* L 202/1, 8 June, pp. 1–31.

CTAC (2023) *CTAC 2023 yearly report*. Regional Cyber Defence Centre, Lithuania.

DataReportal (2024a) *Digital 2024: global overview report*. Available at: https://datareportal.com/reports/digital-2024-global-overview-report (Accessed: 19 September 2025).

DataReportal (2024b) *Digital 2024: Lithuania*. Available at: https://datareportal.com/reports/digital-2024-lithuania (Accessed: 19 September 2025).

Downer, K. and Bhattacharya, M. (2022) 'BYOD security: a study of human dimensions', *Informatics*, 9(1), article 16. Available at: https://doi.org/10.3390/informatics9010016

European Commission (2023) *Shaping Europe's digital future: Cyber Resilience Act*. Available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act (Accessed: 19 September 2025).

Fezzey, T., Batchelor, J.H., Burch, G.F. and Reid, R. (2023) 'Cybersecurity continuity risks: lessons learned from the COVID-19 pandemic', *Journal of Cybersecurity Education, Research & Practice*, 2022(2). Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2022/iss2/4/?utm_source=digitalcommons.kennesaw.edu%2Fjcerp%2Fvol2022%2Fiss2%2F4&utm_medium=PDF&utm_campaign=PDFCoverPages (Accesssed: 11 August 2025).

FinancesOnline (2024) *44 basic BYOD statistics: 2024 market share analysis & data*. Available at: https://financesonline.com/byod-statistics/ (Accessed: 19 September 2025).

Franco, M.F., Künzler, F., von der Assen, J., Feng, C. and Stiller, B. (2024) 'RCVaR: an economic approach to estimate cyberattacks costs using data from industry reports', *Computers & Security*, 139, article 103737. Available at: https://doi.org/10.1016/j.cose.2024.103737

Ganiyu, S.O. and Jimoh, R.G. (2018) 'Characterising risk factors and countermeasures for risk evaluation of Bring Your Own Device strategy', *International Journal of Information Security Science*, 7(1), pp. 49–59. Available at: https://www.researchgate.net/publication/342361828_Characterising_Risk_Factors_and_Countermeasures_for_Risk_Evaluation_of_Bring_Your_Own_Device_Strategy (Accessed: 11 August 2025).

Harthy, K.A. (2022) *A risk management framework for the BYOD environment*. Doctoral thesis. Coventry University. Available at: https://pure.coventry.ac.uk/ws/portalfiles/portal/80093962/AlHarthy_2022_PhD.pdf (Accessed: 11 August 2025).

Howell, G., Franklin, J.M., Sritapan, V., Souppaya, M. and Scarfone, K. (2023) *Guidelines for managing the security of mobile devices in the enterprise*. NIST Special Publication 800-124r2. US Department of Commerce. Available at: https://doi.org/10.6028/NIST.SP.800-124r2

IBM Security (2023) *Cost of a data breach report 2023*. Available at: https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf (Accessed: 19 September 2025).

Ismail, N. (2017) 'Mobile security in the enterprise', *Information Age*, 16 September. Available at: https://www.information-age.com/mobile-enterprise-security-7731/ (Accessed: 19 September 2025).

Jayarao, G.B., Ray, S. and Panigrahi, P.K. (2024) 'Information security threats and organizational readiness in nWFH scenarios', *Computers & Security*, 140, article 103745. Available at: https://doi.org/10.1016/j.cose.2024.103745

Ma, Y., Cao, Y., Li, L., Zhang, J. and Prince Clement, A. (2021) 'Following the flow: exploring the impact of mobile technology environment on user's virtual experience and behavioral response', *Journal of Theoretical and Applied Electronic Commerce Research*, 16(2), pp. 170–187. Available at: https://doi.org/10.4067/S0718-18762021000200112

Mierzwa, S.J. and Klepacka, A. (2023) 'Practical approaches and guidance to small business organization cyber risk and threat assessments', *Journal of Strategic Innovation & Sustainability*, 18(2). Available at: https://doi.org/10.33423/jsis.v18i2.6255

National Cyber Security Centre UK (2020) *Cyber security: small business guide*. Available at: https://www.ncsc.gov.uk/files/NCSC_A5_Small_Business_Guide_v4_OCT20.pdf (Accessed: 19 September 2025).

Center for Internet Security (2017) *CIS Controls implementation guide for small- and medium-sized enterprises (SMEs)*. Available at: https://www.cisecurity.org/-/media/project/cisecurity/cisecurity/data/media/files/uploads/2017/09/CIS-Controls-Guide-for-SMEs.pdf (Accessed: 19 September 2025).

Palanisamy, R., Norman, A.A. and Mat Kiah, L. (2021) 'BYOD security risks and mitigation strategies: insights from IT security experts', *Journal of Organizational Computing & Electronic Commerce*, 31(4), pp. 320–342. Available at: https://doi.org/10.1080/10919392.2022.2028530

Podvezko, V. (2005) 'Agreement of expert estimates', *Technological and Economic Development of Economy*, 11(2), pp. 101–107. Available at: https://doi.org/10.3846/13928619.2005.9637688

Porter, M.E. (1985) *Competitive advantage: creating and sustaining superior performance*. The Free Press.

Rathnayaka, R.P.P.S., Swarnamali, I.S., Piyasekara, W.D.C., Karunathilaka, N.A., Abewardena, K.Y. and Yapa, K. (2023) 'Enhancing security in a corporate BYOD environment', *International Research Journal of Innovations in Engineering and Technology*, 7(11), pp. 329–334. Available at: https://doi.org/10.47001/IRJIET/2023.711045

Research and Markets (2020) *Report*. Available at: https://www.researchandmarkets.com/?srsltid=AfmBOoqdV1dZk4GfDUGZFbCSwxlMuZVFHU6ptbytv298PQLt5F_7PSlh (Accessed: 19 September 2025).

Research and Markets (2025) *BYOD and enterprise mobility: global strategic business report*. Available at: https://www.researchandmarkets.com/reports/4804695/byod-and-enterprise-mobility-global-strategic (Accessed: 19 September 2025).

StrongDM (2024) *Small business cyber security statistics for 2024*. Available at: https://www.strongdm.com/blog/small-business-cyber-security-statistics (Accessed: 19 September 2025).

Sukumar, A., Mahdiraji, H.A. and Jafari-Sadeghi, V. (2023) 'Cyber risk assessment in small and medium-sized enterprises: a multilevel decision-making approach for small e-tailors', *Risk Analysis: An International Journal*, 43(10), pp. 2082–2098. Available at: https://doi.org/10.1111/risa.14092

UK Government (2025) *Cyber security breaches survey 2025*. Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025 (Accessed: 19 September 2025).

Van de Weijer, S., Leukfeldt, R. and Moneva, A. (2023) 'Cybercrime during the COVID-19 pandemic: prevalence, nature and impact of cybercrime for citizens and SME owners in the Netherlands', *Computers & Security*, 139, article 103693. Available at: https://doi.org/10.1016/j.cose.2023.103693

Verizon (2024) *Data breach investigations report*. Available at: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf (Accessed: 19 September 2025).

Wang, J., Ho, C.Y. and Shan, Y.G. (2024) 'Does cybersecurity risk stifle corporate innovation activities?' *International Review of Financial Analysis*, 93, article 103028. Available at: https://doi.org/10.1016/j.irfa.2023.103028

Wiechetek, Ł. and Mędrek, M. (2018) 'Synergizing logistics processes and process management—framework of BPM course based on business cases, BPM standards and tools', *Annales H-Oeconomia*, 52(5), pp. 95–112. Available at: https://doi.org/10.17951/h.2018.52.5.95-112

Zuhaira, B. and Ahmad, N. (2021) 'Business process modeling, implementation, analysis, and management: the case of business process management tools', *Business Process Management Journal*, 27(1), pp. 145–183. Available at: https://doi.org/10.1108/BPMJ-06-2018-0168

Drazich, B.F., Lee, J.W., Bowles, K.H., Taylor, J.L., Shah, S., Resnick, B., Kim, N., and Szanton, S.L. (2023) 'Pandemic-related changes in technology use among a sample of previously hospitalized older adult New Yorkers: observational study', *JMIR Aging*, 6, article e41692. Available at: https://doi.org/10.2196/41692